**Advisory**
Al-Qaeda Intent to Conduct Computer Network Attacks Against Financial Institutions
July 18, 2003

**ATTENTION:** Security Directors, Chief Information Officers, Personnel Security Officers, and Physical Security Officers

## OVERVIEW

Recent reporting continues to underscore Al-Qaeda's interest in undermining U.S. financial institutions.

## DETAILS

Although the federal government possesses only limited direct information indicating that Al-Qaeda intends to conduct computer network attacks against U.S. financial institutions, financial services providers should remain alert to the potential that Al-Qaeda operatives placed in the U.S. may be used to facilitate attacks against financial institutions.

Reporting indicates that Al-Qaeda leaders have operatives in the United States researching "hacking into the mainframes of U.S. banks." This research focused on the feasibility of accessing computers of U.S. banks to wipe off balances and alter records to create instability in the U.S. economy. Al-Qaeda interest in computer science programs at U.S. educational institutions has also been observed.

The apparent interest in the study of computer network attack techniques focused on the financial services sector possibly indicates that Al-Qaeda is developing operatives who understand both computer security and U.S. financial institutions. The Department of Homeland Security's assessment is that such operatives could pose significant threats to the integrity of the infrastructure if they were to gain privileged access as an insider, or indirectly through hacking.

## SUGGESTED PROTECTIVE MEASURES

The following measures are suggested as means for mitigating the potential impact of this threat:

- Vet the backgrounds of all employee candidates – this is especially important for candidates requiring access to the most sensitive information and mission-critical systems.
- Ensure spaces containing mission-critical systems are physically segregated from general work spaces and entry to the former is secured by access-control systems.
- Ensure employees wear clearly visible, tamper-resistant access/identification badges, preferably color coded to signify levels, or extent, of their access to critical systems.
- Ensure all employees enter general work spaces through designated access points. After normal working hours, access points should be reduced to the minimum

necessary and access to internal spaces should be restricted commensurate with the sensitivity or criticality of the items those spaces contain.

- Restrict roles and limit privileges to ensure individuals do not have access or control beyond what they need to perform their authorized functions.
- Configure information systems and networks to be secure and ensure they stay secure (e.g., deactivate unnecessary services, keep software patches up-to-date, and enforce use of secure passwords).
- Monitor information systems and networks for unauthorized insider activity.
- Upon detecting such unauthorized activity, take appropriate action to notify the necessary authorities and officials (e.g., human resources, legal, law enforcement, counterintelligence entities, as appropriate).
- Ensure emergency/contingency plans are written, up-to-date, and approved by management. Such plans should include extra security responders to augment normal security personnel during emergencies and should provide for emergency back-up communications. Plans should be tested on a recurring schedule.

The suggested protective measures above are meant to stimulate constructive organizational dialog on threats and vulnerabilities and are not a substitute for a security risk management program conducted by properly-trained and experienced security professionals and tailored to the requirements of a specific organization.

**Advisories recommend the immediate implementation of protective actions, including best practices when available. DHS encourages recipients of this advisory to report information concerning suspicious or criminal activity to law enforcement or a DHS watch office. The DHS Information Analysis and Infrastructure Protection watch offices may be contacted at:**

| | |
|---|---|
| **For Private citizens and companies –** | **Phone: (202) 323-3205, 1-888-585-9078** |
| | **Email: nipc.watch@fbi.gov** |
| | **Online: http://www.nipc.gov/incident/cirr.htm** |
| **For Telecom industry -** | **Phone: (703) 607-4950** |
| | **Email: ncs@dhs.gov** |
| **For Federal agencies/departments -** | **Phone: (888) 282-0870** |
| | **Email: fedcirc@fedcirc.gov** |
| | **Online: https://incidentreport.fedcirc.gov** |

**DHS intends to update this alert should it receive additional relevant information, including information provided to it by the user community. Based on this notification, no change to the Homeland Security Advisory System (HSAS) is anticipated; the current HSAS level is YELLOW.**